Web Results **1** - **8** of about **13** for "**permutation specification**" **cryptography**. (**0.26** seconds)

Tip: Save time by hitting the return key instead of clicking on "search"

[PDF] Scan Based Side Channel Attack on Data Encryption Standard
File Format: PDF/Adobe Acrobat - View as HTML
From DES initial **permutation specification** [8]: ... [3] J. Goodman. and A.P.. Chandrakasan, An. Energy-Efficient Reconfigurable Public-Key **Cryptography** ...
eprint.iacr.org/2004/083.pdf - Similar pages

[PDF] Scan based side channel attack on dedicated hardware ...
File Format: PDF/Adobe Acrobat
17r1gr19r1r20r1r22r3r2r4r2r2d2r2r29r2r9r3d31r32r1. (7). From DES initial **permutation specification** ... Efficient Reconfigurable Public-Key **Cryptography** ...
ieeexplore.ieee.org/iel5/9526/30190/01386969.pdf - Similar pages

Efficient Permutation Instructions for Fast Software **Cryptography**
This capability results in much faster **cryptography** and multimedia ... second source register can hold only n bits of **permutation specification** and it takes ...
doi.ieeecomputersociety.org/10.1109/40.977759 - Similar pages

[PDF] Scan Based Side Channel Attack on Dedicated Hardware ...
File Format: PDF/Adobe Acrobat
From DES initial **permutation specification** [8]: ... Efficient Reconfigurable Public-Key **Cryptography**. Processor, IEEE Journal of Solid-State Circuits, pp. ...
doi.ieeecomputersociety.org/10.1109/ITC.2004.157 - Similar pages

Automated permutation method and apparatus - Patent 20050036608
The method of claim 1 wherein the first **permutation specification** specifies ... [0002] **Cryptography** involves the enciphering and deciphering of messages in ...
www.freepatentsonline.com/20050036608.html - 45k - Cached - Similar pages

[PDF] Scan Based Side Channel Attack on Dedicated Hardware ...
File Format: PDF/Adobe Acrobat - View as HTML
From DES initial **permutation specification** [8]: ... **Cryptography**. Processor, IEEE Journal of Solid-State Circuits, pp. 1808-. 1820, November, 2001. ...
www.itcprogramdev.org/itc2004proc/Papers/PDFs/0012_2.pdf - Similar pages

EP1388230 Fraunhofer european software patent - Method and device ...
means for applying the permuted vector as a **permutation specification** to an ordered vector of numbers from 1 to N to obtain the permutation vector. ...
gauss.ffii.org/PatentView/EP1388230 - 59k - Cached - Similar pages

US Pregrant 20050036608 - Automated permutation method and apparatus
A second **permutation specification** of a second permutation of the first plurality of inputs is generated, the second permutation ... Class 380, **CRYPTOGRAPHY** ...
cxp.paterra.com/uspregrant20050036608.html - 11k - Supplemental Result - Cached - Similar pages

In order to show you the most relevant results, we have omitted some entries very similar to the 8 already displayed.
If you like, you can repeat the search with the omitted results included.

"permutation specification" cryptogr Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google

Published before April 2003
Terms used
configuring cryptographic unit; permutation specification

Found **30** of **140,683**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 30 Result page: **1** 2 next

Relevance scale

1 CryptoManiac: a fast flexible architecture for secure communication

Lisa Wu, Chris Weaver, Todd Austin
May 2001 **ACM SIGARCH Computer Architecture News , Proceedings of the 28th annual international symposium on Computer architecture ISCA '01**, Volume 29 Issue 2
Publisher: ACM Press

Full text available: pdf(836.04 KB) Additional Information: full citation, abstract, references, citings, index terms

The growth of the Internet as a vehicle for secure communication and electronic commerce has brought cryptographic processing performance to the forefront of high throughput system design. This trend will be further underscored with the widespread adoption of secure protocols such as secure IP (IPSEC) and virtual private networks (VPNs).

In this paper, we introduce the CryptoManiac processor, a fast and flexible co-processor for cryptographic workloads. Our design is extreme ...

2 Architectural support for fast symmetric-key cryptography

Jerome Burke, John McDonald, Todd Austin
November 2000 **ACM SIGOPS Operating Systems Review , ACM SIGARCH Computer Architecture News , Proceedings of the ninth international conference on Architectural support for programming languages and operating systems ASPLOS-IX**, Volume 34 , 28 Issue 5 , 5
Publisher: ACM Press

Full text available: pdf(160.25 KB) Additional Information: full citation, abstract, references, citings, index terms

The emergence of the Internet as a trusted medium for commerce and communication has made cryptography an essential component of modern information systems. Cryptography provides the mechanisms necessary to implement accountability, accuracy, and confidentiality in communication. As demands for secure communication bandwidth grow, efficient cryptographic processing will become increasingly vital to good system performance.In this paper, we explore techniques to improve the performance of symmetr ...

3 Computing curricula 2001

September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press

Full text available: pdf(613.63 KB) Additional Information: full citation, references, citings, index terms

html(2.78 KB)

4 Death, taxes, and imperfect software: surviving the inevitable

Crispin Cowan, Calton Pu

January 1998 **Proceedings of the 1998 workshop on New security paradigms NSPW '98**

Publisher: ACM Press

Full text available: pdf(1.09 MB) Additional Information: full citation, references, index terms

5 Software protection and simulation on oblivious RAMs

Oded Goldreich, Rafail Ostrovsky

May 1996 **Journal of the ACM (JACM)**, Volume 43 Issue 3

Publisher: ACM Press

Full text available: pdf(3.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if thhe sequence in wh ...

Keywords: pseudorandom functions, simulation of random access machines, software protection

6 Verifying security protocols with Brutus

E. M. Clarke, S. Jha, W. Marrero

October 2000 **ACM Transactions on Software Engineering and Methodology (TOSEM)**, Volume 9 Issue 4

Publisher: ACM Press

Full text available: pdf(347.12 KB) Additional Information: full citation, abstract, references, citings, index terms

Due to the rapid growth of the "Internet" and the "World Wide Web" security has become a very important concern in the design and implementation of software systems. Since security has become an important issue, the number of protocols in this domain has become very large. These protocols are very diverse in nature. If a software architect wants to deploy some of these protocols in a system, they have to be sure that the protocol has the right properties as dictated ...

Keywords: authentication and secure payment protocols, formal methods, model-checking

7 Towards a theory of software protection and simulation by oblivious RAMs

O. Goldreich

January 1987 **Proceedings of the nineteenth annual ACM conference on Theory of computing STOC '87**

Publisher: ACM Press

Full text available: pdf(1.32 MB) Additional Information: full citation, abstract, references, citings, index terms

Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we make the first steps towards a theoretic treatment of software protection: First, we distill and

formulate the key problem of learning about a program from its execution. Second, assuming the existence of one-way permutations, w ...

8 On randomization in sequential and distributed algorithms

Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Publisher: ACM Press

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

9 Performance analysis of MD5

Joseph D. Touch
October 1995 **ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Applications, technologies, architectures, and protocols for computer communication SIGCOMM '95**, Volume 25 Issue 4
Publisher: ACM Press

Full text available: pdf(1.04 MB) Additional Information: full citation, abstract, references, citings, index terms

MD5 is an authentication algorithm proposed as the required implementation of the authentication option in IPv6. This paper presents an analysis of the speed at which MD5 can be implemented in software and hardware, and discusses whether its use interferes with high bandwidth networking. The analysis indicates that MD5 software currently runs at 85 Mbps on a 190 Mhz RISC architecture, a rate that cannot be improved more than 20-40%. Because MD5 processes the entire body of a packet, this data ra ...

10 Special session on security on SoC: Securing wireless data: system architecture challenges

Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally
October 2002 **Proceedings of the 15th international symposium on System Synthesis ISSS '02**
Publisher: ACM Press

Full text available: pdf(172.35 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of current and future wireless data applications and services. This paper highlights the challenges posed by the need for security during system architecture design for wireless handsets, and provides an overview of emerging techniques to address them. We focus on the computational requirements for securing wireless data transactions, revealing a gap between these requirements and the trends in processing capabilities of embedded processors used in wireless h ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, WTLS, decryption, design methodology, embedded system, encryption, handset, mobile computing, performance, platform, security, security processing, system architecture, wireless communications

11 Adaptively secure multi-party computation

Ran Canetti, Uri Feige, Oded Goldreich, Moni Naor

July 1996 **Proceedings of the twenty-eighth annual ACM symposium on Theory of computing STOC '96**

Publisher: ACM Press

Full text available: pdf(1.50 MB) Additional Information: full citation, references, citings, index terms

12 Reversible logic circuit synthesis

Vivek V. Shende, Aditya K. Prasad, Igor L. Markov, John P. Hayes

November 2002 **Proceedings of the 2002 IEEE/ACM international conference on Computer-aided design ICCAD '02**

Publisher: ACM Press

Full text available: pdf(246.56 KB) Additional Information: full citation, abstract, references, citings, index terms

Reversible or information-lossless circuits have applications in digital signal processing, communication, computer graphics and cryptography. They are also a fundamental requirement in the emerging field of quantum computation. We investigate the synthesis of reversible circuits that employ a minimum number of gates and contain no redundant input-output line-pairs (temporary storage channels). We prove constructively that every even permutation can be implemented without temporary storage using ...

13 Development of processors and communication networks for embedded systems: System design methodologies for a wireless security processing platform

Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally, Murugan Sankaradass

June 2002 **Proceedings of the 39th conference on Design automation DAC '02**

Publisher: ACM Press

Full text available: pdf(207.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Security protocols are critical to enabling the growth of a wide range of wireless data services and applications. However, they impose a high computational burden that is mismatched with the modest processing capabilities and battery resources available on wireless clients. Bridging the security processing gap, while retaining sufficient programmability in order to support a wide range of current and future security protocol standards, requires the use of novel system architectures and design m ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, decryption, design methodology, embedded system, encryption, handset, performance, platform, security, security processing, system architecture, wireless

14 Fundamentals of computing (a cheatlist)

Leonid A. Levin

September 1996 **ACM SIGACT News**, Volume 27 Issue 3

Publisher: ACM Press

Full text available: pdf(1.76 MB) Additional Information: full citation, index terms

15 Learning read-once formulas with queries

Dana Angluin, Lisa Hellerstein, Marek Karpinski

January 1993 **Journal of the ACM (JACM)**, Volume 40 Issue 1

Publisher: ACM Press

Full text available: pdf(1.97 MB) Additional Information: full citation, abstract, references, citings, index terms

A read-once formula is a Boolean formula in which each variable occurs, at most, once. Such formulas are also called &mgr;-formulas or Boolean trees. This paper treats the problem of exactly identifying an unknown read-once formula using specific kinds of queries. The main results are a polynomial-time algorithm for exact identification of monotone read-once formulas using only membership queries, and a polynomial-time algorithm for exact identification of general read-once formu ...

Keywords: &mgr;-formulas, equivalence queries, exact identification, interpolation, membership queries, polynomial-time learning, read-once formulas

16 Multithreading II: Microarchitectural denial of service: insuring microarchitectural fairness

Dirk Grunwald, Soraya Ghiasi

November 2002 **Proceedings of the 35th annual ACM/IEEE international symposium on Microarchitecture MICRO 35**

Publisher: IEEE Computer Society Press

Full text available: pdf(996.00 KB) Publisher Site

Additional Information: full citation, abstract, references, citings, index terms

Simultaneous multithreading seeks to improve the aggregate computation bandwidth of a processor core by sharing resources such as functional units, caches, TLB and so on. To date, most research investigating the scheduling of these shared resources has focused on enhancing computational bandwidth. In this paper, we examine *scheduling fairness.* First, we show that a thread running on an implementation of a SMT processor can suffer from "denial of service" by a malicious thread, slowing dow ...

17 Atomicity and isolation for transactional processes

Heiko Schuldt, Gustavo Alonso, Catriel Beeri, Hans-Jörg Schek

March 2002 **ACM Transactions on Database Systems (TODS)**, Volume 27 Issue 1

Publisher: ACM Press

Full text available: pdf(1.22 MB)

Additional Information: full citation, abstract, references, citings, index terms

Processes are increasingly being used to make complex application logic explicit. Programming using processes has significant advantages but it poses a difficult problem from the system point of view in that the interactions between processes cannot be controlled using conventional techniques. In terms of recovery, the steps of a process are different from operations within a transaction. Each one has its own termination semantics and there are dependencies among the different steps. Regarding c ...

Keywords: Advanced transaction models, business process management, electronic commerce, execution guarantees, locking, rocesses, semantically rich transactions, transactional workflows, unified theory of concurrency control and recovery

18 Applications of combinatorial designs in computer science

Charles J. Colbourn, Paul C. van Oorschot

June 1989 **ACM Computing Surveys (CSUR)**, Volume 21 Issue 2

Publisher: ACM Press

Full text available: pdf(2.99 MB)

Additional Information: full citation, abstract, references, citings, index terms, review

The theory of combinatorial designs has been used in widely different areas of computation concerned with the design and analysis of both algorithms and hardware. Combinatorial designs capture a subtle balancing property that is inherent in many difficult problems and hence can provide a sophisticated tool for addressing these problems. The role of combinatorial designs in solving many problems that are basic to the field of computing is explored in this paper. Case studies of many applicat ...

19 SPINS: security protocols for sensor networks

Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler
September 2002 **Wireless Networks**, Volume 8 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(213.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: SPINS. SPINS has two secure building blocks: SNEP and μTESLA. SNEP includes: data confidentiality, two-party data authentication, and evidence of data freshness. μTESLA provides authenticated broadcast for severely resource-constrained ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

20 An FPGA implementation and performance evaluation of the Serpent block cipher

A. J. Elbirt, C. Paar
February 2000 **Proceedings of the 2000 ACM/SIGDA eighth international symposium on Field programmable gate arrays FPGA '00**

Publisher: ACM Press

Full text available: pdf(674.09 KB) Additional Information: full citation, abstract, references, citings, index terms

With the expiration of the Data Encryption Standard (DES) in 1998, the Advanced Eneryption Standard (AES) development process is well underway. It is hoped that the result of the AES process will be the specification of a new non-classified encryption algorithm that will have the global acceptance achieved by DES as well as the capability of long-term protection of sensitive information. The technical analysis used in determining which of the potential AES candidates will be selected as the ...

Keywords: FPGA, VHDL, algorithm-agility, block cipher, cryptography

Results 1 - 20 of 30 Result page: **1** 2 next

Published before April 2003
Terms used
configuring cryptographic unit; permutation specification

Found **30** of **140,683**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 21 - 30 of 30 Result page: previous 1 **2**

Relevance scale

21 Resettable zero-knowledge (extended abstract)

Ran Canetti, Oded Goldreich, Shafi Goldwasser, Silvio Micali
May 2000 **Proceedings of the thirty-second annual ACM symposium on Theory of computing STOC '00**
Publisher: ACM Press
Full text available: pdf(1.21 MB) Additional Information: full citation, references, citings, index terms

Keywords: concurrent zero-knowledge, identification schemes, public-key cryptography, smart cards, witness-indistinguisable proofs, zero-knowledge

22 How to play ANY mental game

O. Goldreich, S. Micali, A. Wigderson
January 1987 **Proceedings of the nineteenth annual ACM conference on Theory of computing STOC '87**
Publisher: ACM Press
Full text available: pdf(1.29 MB) Additional Information: full citation, abstract, references, citings, index terms

We present a polynomial-time algorithm that, given as a input the description of a game with incomplete information and any number of players, produces a protocol for playing the game that leaks no partial information, provided the majority of the players is honest. Our algorithm automatically solves all the multi-party protocol problems addressed in complexity-based cryptography during the last 10 years. It actually is a completeness theorem for ...

23 Watermarking techniques for intellectual property protection

A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, G. Wolfe
May 1998 **Proceedings of the 35th annual conference on Design automation DAC '98**
Publisher: ACM Press
Full text available: pdf(243.93 KB) Additional Information: full citation, abstract, references, citings, index terms

Digital system designs are the product of valuable effort and know-how. Their embodiments, from software and HDL program down to device-level netlist and mask data, represent carefully guarded intellectual property (IP). Hence, design methodologies based on IP reuse require new mechanisms to protect the rights of IP producers and owners. This paper establishes principles of watermarking-based IP protection, where a

watermark is a mechanism for identificatio ...

Keywords: intellectual property test, system-on-chip test, testing embedded core

24 Encryption-based protection for interactive user/computer communication

Stephen Thomas Kent
September 1977 **Proceedings of the fifth symposium on Data communications SIGCOMM '77**
Publisher: ACM Press

Full text available: pdf(846.33 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper develops a virtual connection model, complete with intruder, for interactive terminal-host communication and presents a set of protection goals that characterize the security that can be provided for a physically unsecured connection. Fundamental requirements for protocols that achieve these goals and the role of encryption in the design of such protocols are examined. Functional and security constraints on positioning of protection protocols in a communication system and the imp ...

25 Secured systems and Ada: a trusted system software architecture

Mark Aldrich
November 1994 **Proceedings of the conference on TRI-Ada '94 TRI-Ada '94**
Publisher: ACM Press
Full text available: pdf(1.25 MB) Additional Information: full citation, abstract, references, index terms

In this paper, we will present an architecture for developing a system reliant upon trusted Ada software, and some of the lessons learned in our having done such a development. Some background on trusted software and the trusted information systems within which such Ada software operates is provided, as well as some theoretical and practical aspects of the use of Ada in developing these systems. The notion of a trusted computing base (TCB) is presented and defined. A generalized trusted sof ...

26 A secure distributed capability based system (extended abstract)

Howard L. Johnson, John F. Koegel, Rhonda M. Koegel
October 1985 **Proceedings of the 1985 ACM annual conference on The range of computing : mid-80's perspective: mid-80's perspective ACM '85**
Publisher: ACM Press
Full text available: pdf(1.22 MB) Additional Information: full citation, references, index terms

Keywords: capability architecture, computer security, distributed system security, network encryption

27 Secure computation with honest-looking parties (extended abstract): what if nobody is truly honest?

Ran Canetti, Rafail Ostrovsky
May 1999 **Proceedings of the thirty-first annual ACM symposium on Theory of computing STOC '99**
Publisher: ACM Press
Full text available: pdf(938.61 KB) Additional Information: full citation, references, index terms

28 Cellular and Cryptographic Applications: FPGA implementation of neighborhood-of-four cellular automata random number generators

Barry Shackleford, Motoo Tanaka, Richard J. Carter, Greg Snider
February 2002 **Proceedings of the 2002 ACM/SIGDA tenth international symposium**

on Field-programmable gate arrays FPGA '02

Publisher: ACM Press

Full text available: pdf(565.95 KB) Additional Information: full citation, abstract, references

Random number generators (RNGs) based upon neighborhood-of-four cellular automata (CA) with asymmetrical, non-local connections are explored. A number of RNGs that pass Marsaglia's rigorous Diehard suite of random number tests have been discovered. A neighborhood size of four allows a single CA cell to be implemented with a four-input lookup table and a one-bit register which are common building blocks in popular field programmable gate arrays (FPGAs). The investigated networks all had periodic ...

Keywords: FPGA, cellular automata, random number generator

29 The proposed new Computing Reviews classification scheme

Anthony Ralston

July 1981 **Communications of the ACM**, Volume 24 Issue 7

Publisher: ACM Press

Full text available: pdf(972.02 KB) Additional Information: full citation, citings, index terms

30 The new (1982) Computing Reviews classification system—final version

Jean E. Sammet, Anthony Ralston

January 1982 **Communications of the ACM**, Volume 25 Issue 1

Publisher: ACM Press

Full text available: pdf(731.04 KB) Additional Information: full citation, citings, index terms